

Probleemoplossing voor SLP Smart Transport op Catalyst 9000 Switches

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u problemen met Smart Licensing Using Policy (SLP) kunt oplossen met Smart Transport op Catalyst 9000 switches.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met dit onderwerp en er vertrouwd mee te zijn:

- Smart Licensing met beleid voor Cisco IOS® XE-apparaten.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1 en latere versies



Opmerking: Raadpleeg de betreffende configuratiehandleiding voor de opdrachten die worden gebruikt om deze functies op andere Cisco-platforms in te schakelen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Smart Licensing Use Policy is een verbeterde versie van Smart Licensing, die is ontworpen met als hoofddoel een licentieoplossing te bieden die ervoor zorgt dat de activiteiten van uw netwerk ononderbroken blijven. In plaats van verstorend te werken, creëert het een compliance-relatie om de hardware- en softwarelicenties die u koopt en gebruikt te verantwoorden.

Voor Smart Licensing-rapportage om goed te functioneren, maakt de Catalyst 9000 switch verbinding met Cisco Smart Software Manager (CSSM) om licentiegebruik te melden. CSSM

fungeert als een gecentraliseerd platform voor het beheer van alle Cisco-softwarelicenties en voor het beoordelen van gebruik, waardoor u beter kunt plannen voor toekomstige licentieregelingen.

Er zijn meerdere topologieën waardoor een Catalyst 9000 switch verbinding kan maken met CSM, maar dit document concentreert zich op de specifieke topologie waarin de switch rechtstreeks is verbonden met CSM. Dit betekent dat de switch in staat moet zijn om een verbinding met CSSM te bereiken en tot stand te brengen, die op het internet wordt gehost.

In deze directe verbindingstopologie zijn er twee transportopties: Smart Transport en Call Home, met Smart Transport als aanbevolen methode. Daarnaast ondersteunt Smart Transport het gebruik van een HTTPS-proxy en maakt het mogelijk een specifieke VRF te selecteren om slimme licentiecommunicatie met CSM te verwerken.

Wanneer u Smart Transport gebruikt, ruilt de Catalyst 9000 switch licentiegebruiksgegevens met CSSM in JavaScript Object Notation (JSON)-indeling in een HTTPS-bericht. Deze informatie, die bekend staat als het RUM Report, wordt door de switch verzonden, en het antwoord van CSSM wordt aangeduid als een ACK.

De minimale rapportagefrequentie voor deze topologie wordt beperkt tot één dag. Dit betekent dat het productgeval niet meer dan één RUM-rapport per dag zal verzenden, waardoor wordt voorkomen dat voor bepaalde licenties een buitensporig aantal rapporten wordt gegenereerd en verzonden. Dit helpt geheugengerelateerde problemen en systeemvertragingen op te lossen die worden veroorzaakt door een overproductie van RUM rapporten.

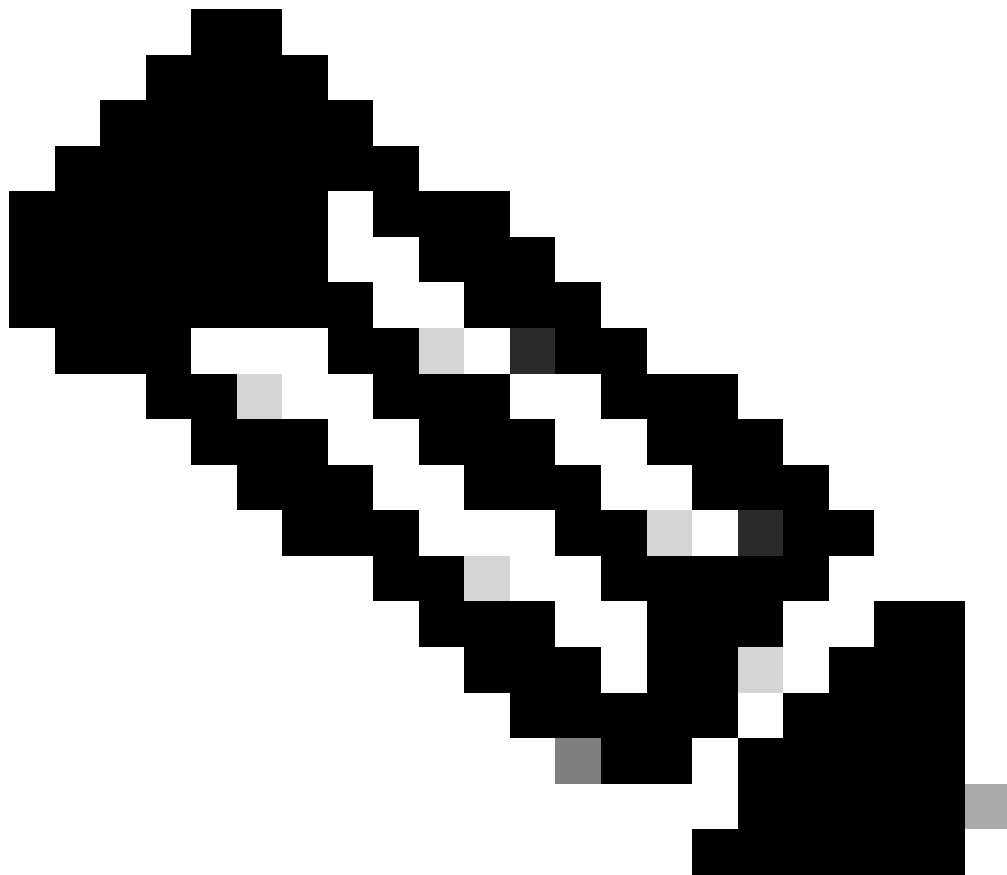
`license smart sync` Indien nodig kunt u deze beperking van throttling negeren door de opdracht in de geprivilegieerde EXEC-modus te gebruiken

Configureren

Volg deze stappen om SLP met slim transport te configureren:

1. Configureer Smart als het transporttype en gebruik de standaard-URL.

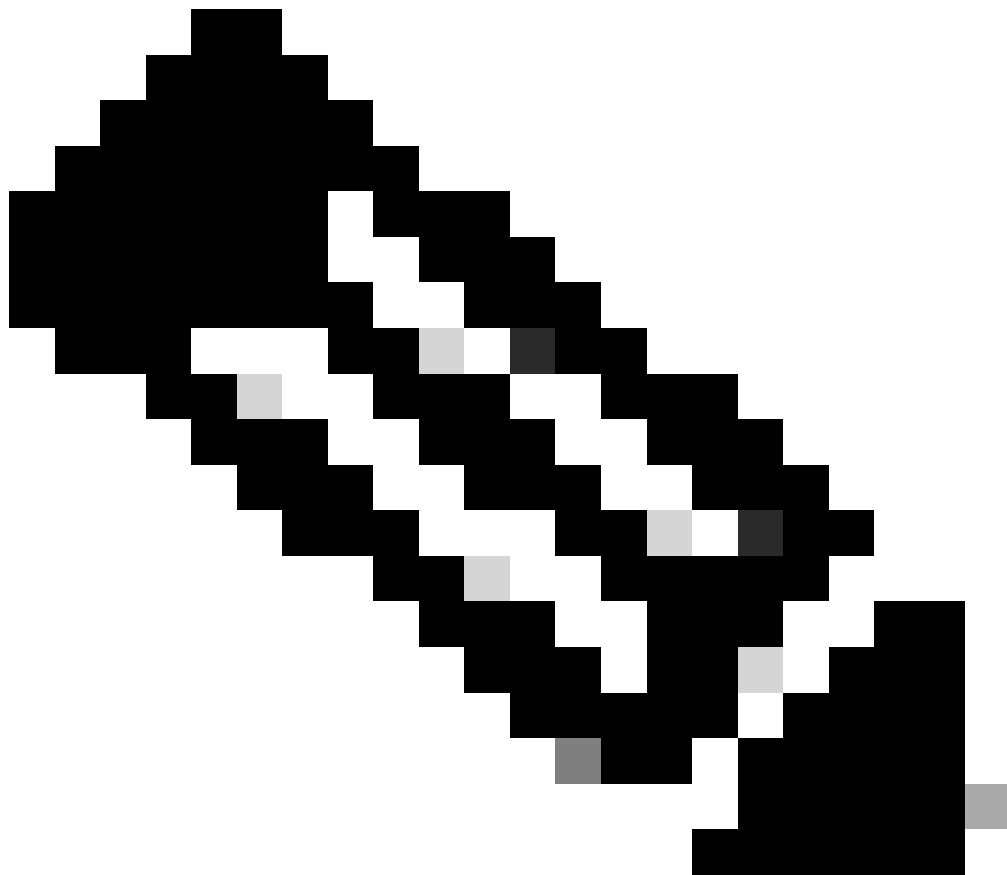
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



Opmerking: Als een VRF wordt gebruikt voor slim transport, moet u dit license smart vrf configureren.

-
2. Configureer de DNS-server en broninterface voor DNS-resolutie en HTTP-clientverbindingen.

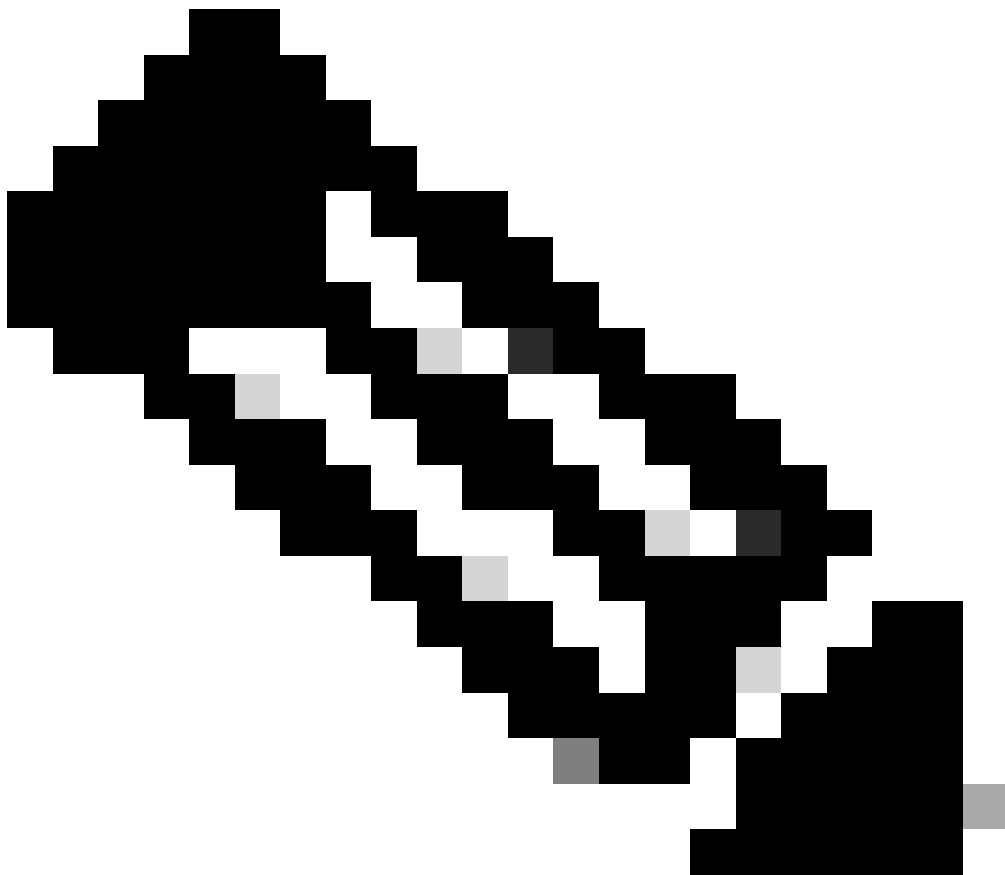
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



Opmerking: Als een VRF wordt gebruikt voor slim transport, moet de VRF-variant van deze opdrachten worden gebruikt.

3. Indien nodig moet u een HTTPS-proxy configureren.

```
Switch(config)#license smart proxy address 192.168.217.105
Switch(config)#license smart proxy port 80
```



Opmerking: De proxyserver kan worden geconfigureerd met zijn IP-adres of hostnaam.

-
4. Genereer een token in de virtuele account. Volg de procedure die in [dit document is](#) beschreven om deze stap te voltooien.
 5. Installeer de vertrouwenscode op de switch.

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDAYNjU5%OA
```

```
[OK]
```

Na een succesvolle vertrouwensinstelling met CSSM wordt een soortgelijke syslog weergegeven.

*Jan 24 23:19:05.144: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully installed.

Bovendien `show license status` toont de tijd van de vertrouwenscode installatie.

<#root>

Switch#show license status | i Trust

Trust Code Installed: Jan 24 23:19:05 2025 UTC

<--- Trust code was installed

Tot slot laat het gebeurtenissenlogboek van de virtuele account zien dat de switch is toegevoegd.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

SL Product Details Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity | Commercial Consumption

Virtual Account: [redacted] 65 Major 440 Minor 54 Informational Hide Alerts

General Licenses Product Instances Event Log

Search by License or Product

Message	Time	User
The product instance "UDI_PID:C9300X-12Y; UDI_SN:[redacted]" connected and was added to the Virtual Account "[redacted]"	2025-Feb-21 17:12:46	System
A new Token "MzgwMDAwMTI0GVkOC00OWExLTgzZmEzMzVhNTZkMDAyNTJhLTE3NDI3NDgy%0ANDkyMTF8U1N4MFV0R..."	2025-Feb-21 16:44:09	[redacted]

Gebeurtenislogboek virtuele account met apparaat.

Problemen oplossen

Als Trust Establishment met CSSM mislukt, wordt een syslog getoond die de reden voor falen aangeeft.

*Jan 24 15:17:46.341: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Manager.

Mogelijke redenen voor communicatiestoringen zijn onder meer:

- Kan serverhostnaam/domeinnaam niet oplossen: De Smart Transport URL of de proxyserver hostnaam is niet opgelost door DNS. Valideer de configuraties van de naamresolutie en bereikbaarheid van de DNS server.

- Time out verbinding: Er werd geprobeerd verbinding te maken, maar er werd geen antwoord ontvangen. Controleer of de HTTPS-verbinding met CSM tot stand wordt gebracht met behulp van pakketopnamen en controleer of een apparaat, zoals een proxyserver of firewall, de connectiviteit blokkeert. Als u een proxyserver gebruikt, zorg er dan voor dat de juiste poort in gebruik is.

Volg deze stappen en validatieopdrachten om SLP met Smart Transport op te lossen:

1. Logboeken van Smart Licensing-gebeurtenissen valideren.

```
<#root>
```

```
Switch#
```

```
show license eventlog 1
```

```
**** Event Log ****
```

```
2025-01-24 13:58:23.900 UTC SAEVT_INIT_START version="5.5.29_re1/114"
2025-01-24 13:58:23.922 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:58:23.922 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:27.620 UTC SAEVT_READY
2025-01-24 13:58:27.621 UTC SAEVT_ENABLED
2025-01-24 13:58:27.665 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2025-01-24 13:58:27.732 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:27.763 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.768 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:30.425 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmInitialize"
2025-01-24 13:58:30.431 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>"
2025-01-24 13:58:30.431 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:37.975 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.062 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2025-01-24 13:58:40.884 UTC SAEVT_HOSTNAME_CHANGE
2025-01-24 13:58:41.734 UTC SAEVT_HA_EVENT eventType="SmartAgentSetNVPairs"
2025-01-24 13:58:42.408 UTC SAEVT_INIT_CONFIG_READ_DONE
2025-01-24 13:58:42.531 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_OIR_AD
2025-01-24 13:58:42.531 UTC SAEVT_HA_CONFIG
2025-01-24 13:58:42.531 UTC SAEVT_HA_UDI udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:42.732 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:42.744 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:43.140 UTC SAEVT_INIT_SYSTEM_INIT
2025-01-24 13:58:44.143 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:59:14.143 UTC SAEVT_INIT_CRYPT0 success="True"
2025-01-24 13:59:14.144 UTC SAEVT_COMM_RESTORED
2025-01-24 13:59:14.176 UTC SAEVT_INIT_COMPLETE
2025-01-24 14:00:14.145 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2025-01-24 14:00:27.432 UTC
```

```
SAEVT_UTILITY_REPORT_START
```

2025-01-24 15:17:46.341 UTC

```
SAEVT_COMM_FAIL error="Connection timed out". <--- Connection timed out
2025-01-24 15:35:22.627 UTC SAEVT_COMM_RESTORED <--- Communication with CSSM restored
```

2. Bevestig connectiviteit met CSSM door te verzenden en een telnet-verbinding te proberen. Hiermee wordt geverifieerd dat er een naamresolutie is en dat er geen beheerblokkering is tussen de switch en CSM.

<#root>

Switch#

```
show ip interface brief | exclude unassigned
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan10	10.31.121.118				
YES	DHCP	up		up	

Switch#

```
ping smartreceiver.cisco.com source Vlan10
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5)

, round-trip min/avg/max = 364/365/368 ms

Switch#

```
telnet smartreceiver.cisco.com 443 /ipv4 /source-interface vlan10
```

Trying X.X.X.X, 80 ...

Open

[Connection to X.X.X.X closed by foreign host]

Als er een proxyserver wordt gebruikt, kunt u dezelfde opdrachten ook proberen via het IP-adres en de poort van de proxyserver.

<#root>

Switch#

```
ping 192.168.217.105
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.217.105, timeout is 2 seconds:  
!!!!
```

```
Success rate is 100 percent (5/5)
```

```
, round-trip min/avg/max = 364/365/368 ms
```

```
Switch#
```

```
telnet 192.168.217.105 80 /ipv4 /source-interface vlan10
```

```
Trying 192.168.217.105, 80 ...
```

```
Open
```

```
[Connection to 192.168.217.105 closed by foreign host]
```

3. Bevestig dat RUM-rapporten worden verzonden en of er een antwoord is.

```
<#root>
```

```
Switch#
```

```
show license history message
```

```
Message History (oldest to newest):
```

```
=====
```

```
Trust Establishment:
```

```
REQUEST: Jan 24 23:18:59 2025 UTC <--- RUM report was sent
```

```
{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300-48UN",
```

```
RESPONSE: Jan 24 23:19:05 2025 UTC <--- Response from CSSM was received
```

```
{"signature":{"type":null,"value":null,"piid":null,"cert_sn":null},"response":{"header":{"vers
```

```
Usage Reporting:
```

```
  No past history
```

```
Result Polling:
```

```
  No past history
```

```
Authorization Request:
```

```
  No past history
```

```
Authorization Return:
```

```
  No past history
```

```
Trust Sync:
```

```
  No past history
```

```
Import Message History (oldest to newest):
```

```
=====
```

```
Import POLICY:
```

```
  No past Import history
```

Import AUTH:
No past Import history

Import TRUST CODE:
Received on Jan 24 23:19:05 2025 UTC
<TRUST_CODE>

Import RUM ACK:
No past Import history

Import CONVERSION ACK:
No past Import history

Import ACCOUNT INFO:
Last policy received on Jan 24 23:19:05 2025 UTC
<ACCOUNT_INFO>

Switch#

show license tech support | sec Trust

Trust Establishment:
Attempts: Total=1,

Success=1

, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:05 2025 UTC <--- Trust establishment succeeded

Failure Reason:

Last Success Time: Jan 24 23:19:05 2025 UTC

Last Failure Time:

Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response:

Failure Reason:

Last Success Time:

Last Failure Time:

Trust Sync:

Attempts: Total=1,

Success=1,

Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:50 2025 UTC

Failure Reason:

Last Success Time: Jan 24 23:19:50 2025 UTC

Last Failure Time:

Trusted Store Interface: True

Local Device: P:C9300-48UN,S:

, state[2], Trust Data INSTALLED TrustId:612

Overall Trust: INSTALLED (2) <--- Trust code installed

show license history message Als er een verzoek wordt verzonden maar er is geen reactie van CSSM, toont het bevel geen JSON gegevens voor de gegeven reactie en meer details over de mislukking kunnen worden verkregen.

<#root>

Switch#

show license history message

! <--- Output omitted for brevity --->
Trust Establishment:

REQUEST: Feb 21 16:54:49 2025 UTC

{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300X-12Y",

RESPONSE: Feb 21 16:54:49 2025 UTC

<--- The line is empty, which means there was no response from CSSM

REQUEST: Feb 21 16:55:19 2025 UTC

{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300X-12Y",
! <--- Output omitted for brevity --->

Switch#

show license tech support | sec Trust

Trust Establishment:
Attempts: Total=2, Success=0,

Fail=2

Ongoing Failure: Overall=2 Communication=2

Last Response: NO REPLY on Feb 21 16:55:39 2025 UTC

<--- Failure reason was NO REPLY

Failure Reason: <none>

Last Success Time: <none>
Last Failure Time: Feb 21 16:55:39 2025 UTC
Trust Acknowledgement:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trust Sync:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trusted Store Interface: True
Local Device: P:C9300-48UN,S:<SN>, state[1],

NOT INSTALLED

TrustId:605

<--- Trust point exists but it is not installed yet

Overall Trust: No ID

4. Schakel de switch in om een RUM-rapport te verzenden om te synchroniseren met CSSM.

<#root>

Switch#

show clock

*23:38:54.683 UTC Fri Jan 24 2025

Switch#

show license tech support | i Utility

Utility:

Start Utility Measurements: Jan 24 23:35:55 2025 UTC (4 minutes, 38 seconds remaining)

Send Utility RUM reports: Feb 23 23:20:56 2025 UTC (29 days, 23 hours, 49 minutes, 39 seconds remaining)

Process Utility RUM reports: Jan 25 23:30:58 2025 UTC (23 hours, 59 minutes, 41 seconds remaining)

Switch#

show license history message | i REQUEST

REQUEST: Jan 24 23:18:59 2025 UTC

REQUEST: Jan 24 23:20:50 2025 UTC

REQUEST: Jan 24 23:25:55 2025 UTC

REQUEST: Jan 24 23:19:41 2025 UTC

Switch#

```
license smart sync all <--- Trigger synchronization
```

```
Switch#
```

```
show license history message | i REQUEST
```

```
REQUEST: Jan 24 23:18:59 2025 UTC  
REQUEST: Jan 24 23:20:50 2025 UTC  
REQUEST: Jan 24 23:25:55 2025 UTC  
REQUEST: Jan 24 23:19:41 2025 UTC
```

```
REQUEST: Jan 24 23:39:05 2025 UTC
```

```
<--- New RUM report was sent
```

```
Switch#
```

```
show license tech support | sec Trust
```

```
Trust Establishment:
```

```
Attempts: Total=1, Success=1, Fail=0 Ongoing Failure: Overall=0 Communication=0  
Last Response: OK on Jan 24 23:19:05 2025 UTC  
Failure Reason:  
Last Success Time: Jan 24 23:19:05 2025 UTC  
Last Failure Time:
```

```
Trust Acknowledgement:
```

```
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0  
Last Response:  
Failure Reason:  
Last Success Time:  
Last Failure Time:
```

```
Trust Sync:
```

```
Attempts:
```

```
Total=2, Success=2
```

```
, Fail=0 Ongoing Failure: Overall=0 Communication=0
```

```
Last Response: OK on Jan 24 23:39:14 2025 UTC <--- Successful response from CSSM
```

```
Failure Reason:  
Last Success Time: Jan 24 23:39:14 2025 UTC  
Last Failure Time:  
Trusted Store Interface: True  
Local Device: P:C9300-48UN,S:<SN>, state[2], Trust Data INSTALLED TrustId:612  
Overall Trust: INSTALLED (2)
```

5. Om te bevestigen dat de switch de HTTPS-verbinding met CSSM tot stand brengt, kunt u een pakketopname nemen. Dit is een voorbeeldpakketopname van een succesvolle verbinding via een proxyserver.

```
<#root>
```

```
Switch#
```

```
sh ip cef 10.31.104.78
```

```
0.0.0.0/0
```

```
nexthop 10.31.121.65 Vlan10
```

```
Switch#
```

```
sh ip arp 10.31.121.65
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.31.121.65	0			

```
2c31.24b1.6bc6
```

```
ARPA Vlan10
```

```
Switch#
```

```
show mac address-table address 2c31.24b1.6bc6
```

Mac Address Table

Vlan	Mac Address	Type	Ports
10	2c31.24b1.6bc6	DYNAMIC	

```
Fi1/0/48
```

```
Total Mac Addresses for this criterion: 1
```

```
Switch#
```

```
monitor capture CSSM interface Fi1/0/48 both match any
```

```
Switch#
```

```
monitor capture CSSM start
```

```
Started capture point : CSSM
```

```
Switch#
```

```
show clock
```

```
*
```

```
15:41:10.058 UTC
```

```
Fri Jan 24 2025
```

```
Switch#
```

```
license smart sync all
```

```
Switch#sh license hist mess | i REQUEST  
REQUEST: Jan 24 15:35:17 2025 UTC
```

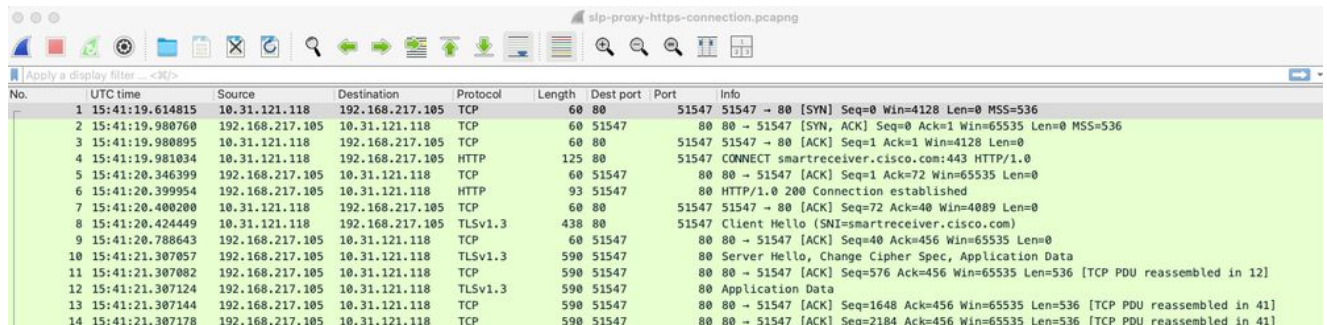
```
REQUEST: Jan 24 15:41:58 2025 UTC
```

```
Switch#
```

```
monitor capture CSSM stop
```

```
Switch#
```

```
monitor capture CSSM export location flash:slp-proxy-https-connection.pcap  
Export Started Successfully
```



The image shows a Wireshark packet capture window titled 'slp-proxy-https-connection.pcap'. The display filter is 'Apply a display filter ... <36>'. The packet list shows 14 packets. The first packet is a SYN from 10.31.121.118 to 192.168.217.105 on port 80. The second packet is a SYN-ACK from 192.168.217.105 to 10.31.121.118 on port 80. The third packet is an ACK from 10.31.121.118 to 192.168.217.105 on port 80. The fourth packet is a CONNECT request from 10.31.121.118 to 192.168.217.105 on port 80. The fifth packet is an ACK from 192.168.217.105 to 10.31.121.118 on port 80. The sixth packet is an HTTP 200 response from 192.168.217.105 to 10.31.121.118 on port 80. The seventh packet is a TLSv1.3 Client Hello from 10.31.121.118 to 192.168.217.105 on port 80. The eighth packet is a TLSv1.3 Server Hello from 192.168.217.105 to 10.31.121.118 on port 80. The ninth packet is a TLSv1.3 Change Cipher Spec from 10.31.121.118 to 192.168.217.105 on port 80. The tenth packet is a TLSv1.3 Application Data from 10.31.121.118 to 192.168.217.105 on port 80. The eleventh packet is a TLSv1.3 Application Data from 192.168.217.105 to 10.31.121.118 on port 80. The twelfth packet is a TLSv1.3 Application Data from 10.31.121.118 to 192.168.217.105 on port 80. The thirteenth packet is a TLSv1.3 Application Data from 192.168.217.105 to 10.31.121.118 on port 80. The fourteenth packet is a TCP RST from 192.168.217.105 to 10.31.121.118 on port 80.

No.	UTC time	Source	Destination	Protocol	Length	Dest port	Port	Info
1	15:41:19.614815	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [SYN] Seq=0 Win=4128 Len=0 MSS=536
2	15:41:19.980760	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536
3	15:41:19.980895	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0
4	15:41:19.981034	10.31.121.118	192.168.217.105	HTTP	125	80	51547	CONNECT smartreceiver.cisco.com:443 HTTP/1.0
5	15:41:20.346399	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=1 Ack=72 Win=65535 Len=0
6	15:41:20.399954	192.168.217.105	10.31.121.118	HTTP	93	51547	80	HTTP/1.0 200 Connection established
7	15:41:20.400200	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=72 Ack=40 Win=4089 Len=0
8	15:41:20.424449	10.31.121.118	192.168.217.105	TLSv1.3	438	80	51547	Client Hello (SNI=smartreceiver.cisco.com)
9	15:41:20.788643	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=40 Ack=456 Win=65535 Len=0
10	15:41:21.307857	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Server Hello, Change Cipher Spec, Application Data
11	15:41:21.307882	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=576 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 12]
12	15:41:21.307124	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Application Data
13	15:41:21.307144	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=1648 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]
14	15:41:21.307178	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=2184 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]

Packet Capture van succesvolle HTTPS-verbinding met CSM met behulp van een proxyserver.

6. Als de pakketopname aantoont dat de HTTPS-verbinding probeert tot stand te worden gebracht maar mislukt, kan dit te wijten zijn aan een falen van een TLS- of SSL-handdruk. Deze debugs kunnen gebruikt worden voor verder onderzoek.

```
debug ip http client all  
debug ssl openssl states  
debug ssl openssl errors  
debug crypto pki messages  
debug crypto pki transactions
```

7. Als de geïnstalleerde vertrouwenscode uit de switch moet worden verwijderd, kan een Smart Licensing-fabrieksreset worden uitgevoerd. Dit proces moet opnieuw worden geladen. Nadat de fabriek is hersteld, kan er een nieuwe vertrouwenscode worden geïnstalleerd. Met deze opdracht wordt alle licentieinformatie, inclusief het beleid, verwijderd.

```
<#root>
```

```
Switch#
```

```
license smart factory reset
```

```
%Warning: reload required after "license smart factory reset" command
```

```
Switch#
```

```
show license status | include Trust
```

```
Trust Code Installed:
```

```
<--- Installed trust code now shows none
```

```
Switch#
```

```
reload
```

Gerelateerde informatie

- [Smart Licensing met beleid voor Cisco Catalyst 9000 Series Switches](#)
- [Intelligente licentiëring voor Catalyst-switching](#)
- [Cisco live: Inleiding tot slimme licentiëring met beleid](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.